

PUBLIC KEY CRYPTOGRAPHY BASED ON SOME EXTENSIONS OF GROUP

Ali Abdallah *

March 14, 2016

Abstract

Bogopolski, Martino and Ventura in [BMV10] introduced a general criteria to construct groups extensions with unsolvable conjugacy problem using short exact sequences. We prove that such extensions have always solvable word problem. This makes the proposed construction a systematic way to obtain finitely presented groups with solvable word problem and unsolvable conjugacy problem. It is believed that such groups are important in cryptography. For this, and as an example, we provide an explicit construction of an extension of Thompson group F and we propose it as a base for a public key cryptography protocol.

1 Introduction

In 1997, Shor in his influential paper [Sho97] proposed a theoretical quantum algorithm for integer factorization into prime numbers that runs in polynomial time. This would, in theory, compromise the current most used public key crypto systems implementations (RSA, ECC, ...). Since then, it is believed that group based cryptography might be a solution in order to provide more secure cryptographic implementation [MSU08]. It is believed also that one solution could be to find group with solvable word problem in linear time and with another very hard decision problem.

The following group decision problems were first introduced by Max Dehn in 1911, within the context of closed 2-manifolds

- The **word problem**: $WP(G) = \{x \in \Omega^* \mid x \stackrel{G}{=} 1\}$.
- The **conjugacy problem**: $CP(G) = \{x, y \in \Omega^* \mid y \stackrel{G}{=} g^{-1}xg, g \in G\}$.

Dehn showed that the word and conjugacy problems for the fundamental group of a closed orientable surface of genus $g \geq 2$ is recursively solvable. Furthermore, he defined the so called **Dehn presentation** for groups for which he gives explicit algorithms for solving the word and conjugacy problems. This is not the case for all finitely generated/presented groups.

Theorem 1 (Novikov [Nov54], Boone [Boo54]) *There exists a finitely presented group whose word problem is recursively unsolvable.*

*Affiliation: Department of Mathematics; University of Rome Tor Vergata

A group with solvable conjugacy problem obviously has solvable word problem, but the converse is not true in general. For example, Fidman [Fri69] in 1960 showed that groups constructed earlier by Novikov in [Nov58] have unsolvable conjugacy and solvable word problem. In this article we will be interested by such groups, but using the technique developed by Bogopolski, Martino and Ventura [BMV10], which permits to construct group that under some conditions will have solvable/unsolvable conjugacy problem. In section 2, we show that these extensions have always solvable word problem. In section 3, we construct an explicit presentation of an extension of Thompson group F with solvable word problem and unsolvable conjugacy problem. Finally, in section 4 we illustrate the application of such extensions to cryptography.

2 Group Extensions with Solvable Word Problem and Unsolvable Conjugacy Problem

Given a short exact sequence of groups

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1. \quad (1)$$

We require that images and pre-images via the morphisms α and β to be computable. The group of interest is the group G , extension of the group F . Under suitable assumptions on the groups F and H , the group G will have solvable or unsolvable conjugacy problem. In addition, we will prove that in both cases the group G will have solvable word problem. Consider the following decidability problems:

- The **orbit decidability problem**. Given a subgroup $A \leq \text{Aut}(F)$, we set

$$\text{OB}(F) = \{(x, y) \in F \times F \mid \varphi(y) = g^{-1}xg, \varphi \in A \text{ and } g \in F\}.$$

- The **φ -twisted conjugacy problem**: For $\varphi \in \text{Aut}(F)$, we set

$$\text{TCP}_\varphi(F) = \{(x, y) \in F \times F \mid y = g^{-1}x\varphi(g)\}.$$

- The **twisted conjugacy problem** $\text{TCP}(F)$: F has solvable twisted conjugacy problem (TCP) if TCP_φ is solvable for every $\varphi \in \text{Aut}(F)$, and unsolvable TCP otherwise.

In the short exact sequence of (1), $\alpha(F)$ is a normal subgroup of G . Thus we can identify F with its image $\alpha(F)$ in G . In addition, every inner automorphism of G ($\varphi_g : G \longrightarrow G$, that maps $x \in G$ to $g^{-1}xg$), restricts to an automorphism of F . We then define the **action subgroup** as follows:

$$A_G = \{\varphi_g \mid g \in G\} \leq \text{Aut}(F).$$

Theorem 2 [BMV10] *Suppose we are given a computable short exact sequence*

$$1 \longrightarrow F \xrightarrow{\alpha} G \xrightarrow{\beta} H \longrightarrow 1$$

with the following requirements:

- i. for every $\varphi \in A_G$, F has solvable φ -twisted conjugacy problem.,
- ii. H has solvable conjugacy problem,
- iii. for every $h \in H$ such that $h \neq 1$, the subgroup $\langle h \rangle$ has a finite index in its centralizer $C_H(h)$.
And a corresponding coset representatives of $\langle h \rangle$ can be computed.

Then:

The conjugacy problem for G is solvable if and only if the action subgroup A_G is orbit decidable.

Theorem 3 Extensions obtained under the conditions of Theorem 2 have solvable word problem.

Proof When the extension group G has solvable conjugacy problem, the solvability of the word problem follows immediately.

Now consider the case when the extension group G has unsolvable conjugacy problem and let $y, y' \in G$, we map them into H , if they are not equal in H , then they cannot be equal in G . Otherwise $\beta(yy'^{-1}) =_H 1$, and there is $f \in F$, such that $\alpha(f) = yy'^{-1}$. Since α is an injective map, it follows that $y =_G y'$ if and only if $f =_F 1$, which we can decide since the word problem of F is solvable. \square

Theorem 2 gives a systematic effective method to construct extensions of the group F with unsolvable/solvable conjugacy problem for which the word problem is solvable.

We need to introduce a new decision problem which we are going to link to the orbit decidability problem. Let B be a group and let A be a subgroup of B . The **membership problem** for A in B is defined as follows:

$$\text{MP}(A, B) = \left\{ b \in B \mid a \in A, b \underset{A}{=} a \right\}$$

That is, given an element $b \in B$ decide whether or not it belongs to A .

Theorem 4 Let $G = \langle x_1, \dots, x_n \mid R_1, \dots, R_m \rangle$ a finitely presented group with unsolvable word problem. Let A be the following subgroup of $F_n \times F_n$

$$A = \left\{ (x, y) \in F_n \times F_n \mid x \underset{G}{=} y \right\} \leq F_n \times F_n$$

Then the membership problem of A in $F_n \times F_n$ is unsolvable.

The construction presented in the above theorem is known as Mihailova's construction and the group A is called the Mihailova subgroup of $F_n \times F_n$ associated with the group G [Mik66].

Let F be a group, the **stabilizer** of a subgroup $A \leq F$ is:

$$\text{Stab}(A) = \{ \varphi \in \text{Aut}(F) \mid \varphi(a) = a, \forall a \in A \} \leq \text{Aut}(F).$$

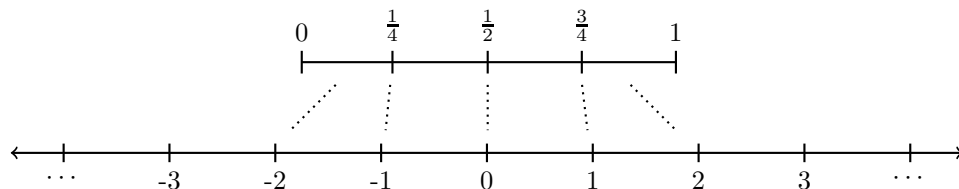
We denote now by $\text{Stab}^*(A) = \text{Stab}(A) \cdot \text{Inn}(F) \leq \text{Aut}(F)$, the **conjugacy stabilizer** of A , where $\text{Inn}(F)$ denotes the group of inner automorphism of F . The notation " \cdot " denotes that elements of $\text{Stab}^*(A)$ are composition of an element of $\text{Stab}(A)$ and of an inner automorphism of F .

Proposition 1 ([BMV10]) Given a group F and two subgroups $A \leq B \leq \text{Aut}(F)$ and an element $v \in F$ such that $B \cap \text{Stab}^*(\langle v \rangle) = \{\text{id}\}$. If $A \leq \text{Aut}(F)$ is orbit decidable then $\text{MP}(A, B)$ is solvable.

Corollary 1 Suppose we are given a finitely presented group with solvable TCP, and such that $F_n \times F_n$ embeds in $\text{Aut}(F)$. If for $v \in F$, $\text{Stab}^*(\langle v \rangle) \cap (F_n \times F_n) = \{\text{id}\}$, then it is possible to construct a finitely presented group with unsolvable CP, but solvable WP.

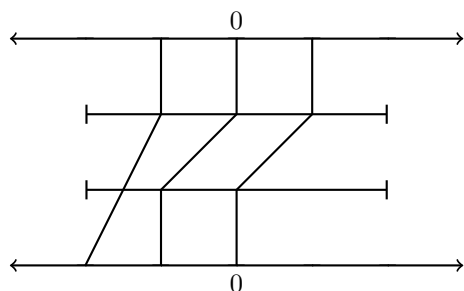
3 Extension of Thompson Group F

The structure of the automorphism group of F was described by Brin in [Bri96]. As it is suggested by Brin, an easy way to understand the automorphisms of F is to look at F as a subgroup of a larger group. For this we introduce the group $\text{PL}_2(\mathbb{R})$ of piece-wise-linear homeomorphisms of the real line, with dyadic breakpoints and power of 2 slopes; allowing this time the set of breakpoints to be infinite, but countable. In order to see F as a subgroup of $\text{PL}_2(\mathbb{R})$, we conjugate elements of F to the real line with a map $\varphi : \mathbb{R} \rightarrow (0, 1)$ that is described in the following figure:

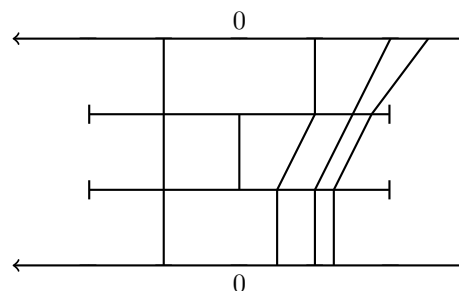


This defines an isomorphism from F to a subgroup of $\text{PL}_2(\mathbb{R})$ which is given by the conjugation map $f \mapsto \varphi^{-1}f\varphi$. With this conjugation, it is easy to see that elements of F can be seen as elements of $\text{PL}_2(\mathbb{R})$, with finitely many break points.

Example 1 We illustrate in the following two diagrams the mapping of A and B , the generators of Thompson group F . For instance the left diagram, which is the mapping of A , can be read from top to bottom as $\varphi \rightarrow A \rightarrow \varphi^{-1}$.



$$\alpha(t) = t - 1$$



$$\beta(t) = \begin{cases} t & t \leq 0 \\ t/2 & 0 \leq t \leq 2 \\ t - 1 & t \geq 2 \end{cases},$$

and α, β generates a subgroup of $\text{PL}_2(\mathbb{R})$, which will be denoted by $\text{PL}_2(I)$.

It follows that any element of the group $g = \varphi^{-1}f\varphi \in \text{PL}_2(\mathbb{R})$, must satisfy the following: $\exists M, N \in \mathbb{R}$ and $k, l \in \mathbb{N}$ such that

- For all $x > M$, $g(x) = x + k$,
- For all $x < N$, $g(x) = x + l$.

The following theorem is the key point to understand $\text{Aut}(F) \cong \text{Aut}(\text{PL}_2(I))$. A complete proof can be found in [Bri96].

Theorem 5 (Brin) *Given $G \leq \text{PL}_2(\mathbb{R})$ we have:*

$$\text{Aut}(G) \cong N(G),$$

where $N(G)$ is the normalizer of G in $\text{PL}_2(\mathbb{R})$.

Viewing F as subgroup of $\text{PL}_2(\mathbb{R})$, the automorphisms of F are elements of $\text{PL}_2(\mathbb{R})$ that conjugate F to itself. Let $\alpha \in \text{Aut}(G) \leq \text{PL}_2(\mathbb{R})$ be a conjugator for f_A . There exists $g \in \text{PL}_2(I)$, such that $f_A \alpha = \alpha g$. Let M be the bounded interval for g , such that $x > M$, $g(x) = x + l$ for some integer l . Take $x > M$, we have $f_A(\alpha(x)) = \alpha(x) - 1 = \alpha g(x) = \alpha(x + l)$. By simply writing down the general equation for α , we can conclude that $l = -1$. It follows that any $\alpha \in \text{Aut}(G)$, must satisfy $\alpha(x + 1) = \alpha(x) + 1$ outside some bounded interval.

In [BMV13] the authors proved that the twisted conjugacy problem is solvable for Thompson group F . They prove the existence of extensions of Thompson group F with unsolvable conjugacy problem. We do the proof for the extensions construction parts in a slightly different way, because it is helpful in constructing an explicit presentation of F .

Theorem 6 (Burillo, Matucci, Ventura [BMV13]) *The twisted conjugacy problem is recursive for Thompson's group F .*

The group $\text{PL}_2(\mathbb{R})$ contains an index two subgroup, namely the subgroup of orientation preserving maps, usually denoted by $\text{PL}_2^+(\mathbb{R})$ and the subgroup of orientation reversing maps, usually denoted by $\text{PL}_2^-(\mathbb{R})$. In the same way, $\text{Aut}^+(F)$ denotes the subgroup of automorphisms of F that preserve the orientation. This is important as we are going to work only with orientation preserving automorphism to obtain a short exact sequence between F , $\text{Aut}^+(F)$ and $T \times T$. We recall that Thompson group T is the group of piece-wise linear homeomorphisms of $S^1 = [0, 1]/\{0 = 1\}$ which are differentiable with derivatives equal to powers of 2, except on a finite set of dyadic rational numbers of the form $p/2^q$.

Now by regarding S^1 as \mathbb{R}/\mathbb{Z} we can view Thompson group T as $\text{PL}_2(\mathbb{R}/\mathbb{Z})$. For an element $a \in \text{Aut}^+(F)$ we have $a(x + 1) = a(x) + 1$ outside of some bounded interval $[M, N]$, we can map $a|_{(k-1, k]}$ for some $k < M$ to the quotient modulo \mathbb{Z} to obtain an element of T . In the same way, we map $a|_{[l, l+1)}$ to an element of T for some $l > N$. We denote this mapping by $\beta(a) = (a_-, a_+)$.

Proposition 2 *There is a short exact sequence:*

$$1 \longrightarrow F \xrightarrow{i} \text{Aut}^+(F) \xrightarrow{\beta} T \times T \longrightarrow 1,$$

where i is the inclusion map.

Proof Identifying F with its image $i(F)$ in $\text{Aut}^+(F)$, we can see that an element $f \in i(F)$ ($\exists M; x > M, f(x) = x + k$, and $\exists N; x < N, f(x) = x + l$) gets mapped to the identity by β , these elements are exactly $\ker(\beta)$.

We shall see that β is surjective. Fix $p < q \in \mathbb{R}$, for $t = (t_-, t_+) \in T \times T$, and let \widetilde{t}_- and \widetilde{t}_+ be a periodic lifting of t_- and t_+ respectively such that $\widetilde{t}_-(p - 1) < p$ and $q < \widetilde{t}_+(q + 1)$. Next we compute $g_-, g, g_+ \in F$ such that $g_-(p - 1) = \widetilde{t}_-(p - 1)$, $g_-(p) = p$, $g(p) = p$, $g(q) = q$ and

$$g_+(q) = q, g_+(q+1) = \widetilde{t_+}(x).$$

$$a(x) = \begin{cases} \widetilde{t_-}(x) & x \leq p-1 \\ g_-(x) & p-1 \leq x \leq p \\ g(x) & p \leq x \leq q \\ g_+(x) & q \leq x \leq q+1 \\ \widetilde{t_+}(x) & q+1 \leq x, \end{cases}$$

It is clear that $a \in \text{Aut}^+(F)$ and $\beta(a) = t = (t_-, t_+)$. \square

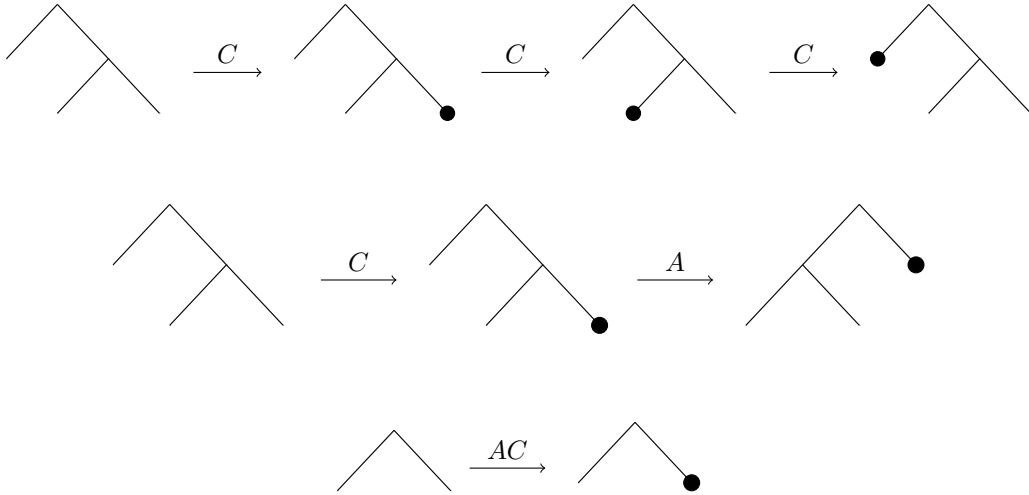
Theorem 7 For every free subgroup $F_2 \leq T$ of rank 2, there is an extension of Thompson group F with solvable word problem and unsolvable conjugacy problem.

Proof Let $F_2 \cong \langle u, v \rangle \leq T$ a free group of rank 2 in T . We construct the following free product $F_2 \times F_2 \cong \langle a, b \rangle \times \langle c, d \rangle \leq T \times T$, where $a = u^2, b = v^2, c = uvu^{-1}$ and $d = vuv^{-1}$.

We construct lifts $\hat{a}, \hat{b}, \hat{c}, \hat{d}$ of a, b, c and d respectively such that $\beta(\hat{a}) = (a, 1), \beta(\hat{b}) = (b, 1), \beta(\hat{c}) = (1, c)$ and $\beta(\hat{d}) = (1, d)$. By construction this gives a copy $B := F_2 \times F_2 \cong \langle \hat{a}, \hat{b}, \hat{c}, \hat{d} \rangle \leq \text{Aut}^+(F)$.

Now in order to conclude the proof, we need to show that for some $v \in F$ one has $B \cap \text{Stab}^*(v) = \{\text{id}\}$. For that let $v \in F, v(x) = x+1, \forall x \in \mathbb{R}$ and let $s \in B \cap \text{Stab}^*(v)$. Since s acts on F by conjugation, we have $s^{-1}vs = g^{-1}vg$ for some $g \in F$, thus sg^{-1} and v commutes. Since v is periodic of period 1 over the entire real line, it follows that $\beta(sg^{-1}) = (t, t) = \beta(s)$, for some $t \in T$. By writing down s in terms of reduced words over $sg^{-1} = w_1(\hat{a}, \hat{b})w_2(\hat{c}, \hat{d}) \in \langle \hat{a}, \hat{b}, \hat{c}, \hat{d} \rangle$, we can conclude that $\beta(s) = (t, t)$ can only happen if and only if $t = 1_T$. And so $B \cap \text{Stab}^*(v) = \{\text{id}\}$. Therefore we can apply Theorem 1 to obtain an extension with solvable word problem and unsolvable conjugacy problem. \square

It is known that Thompson group F does not contain a subgroup which is isomorphic to the free group of rank 2. Unlike Thompson group F , the group T contains free subgroups of rank 2. This implies the existence of extensions of F with unsolvable conjugacy problem.



From the computation presented in the above diagrams, the following equations hold in T :

- i. $C^3 = 1$,
- ii. $(AC)^2 = 1$.

In order to find a copy of F_2 in T , we view Thompson group T as the group of orientation preserving homeomorphisms of the real projective line \mathbb{RP}^1 , which are piecewise $\text{PSL}_2(\mathbb{Z})$ and differentiable except on a finite set of rational numbers. In this way, the group $\text{PSL}_2(\mathbb{Z})$ can be seen as a subgroup of T . The standard presentation of $\text{PSL}_2(\mathbb{Z})$ is:

$$\text{PSL}_2(\mathbb{Z}) = \langle a, b \mid a^2 = b^3 = 1 \rangle$$

Proposition 3 [Fos14] *The subgroup $H = \langle abab^{-1}, ab^{-1}ab \rangle$ is a free non abelian group of rank 2 in T .*

We can explicitly obtain an isomorphic copy of H in T using what we have computed before ($C^3 = (AC)^2 = 1$). Thus the following copy of H in T written as follows

$$H = \langle u = AC^2A, v = A^2C^2 \rangle$$

is a free non abelian group of rank 2 in T . We take $\langle a, b \rangle \times \langle c, d \rangle \leq T \times T$, where $a = u^2, b = v^2, c = uvu^{-1}$ and $d = vuv^{-1}$. And so we have a copy of $F_2 \times F_2 \cong \langle \hat{a}, \hat{b} \rangle \times \langle \hat{c}, \hat{d} \rangle \leq \text{Aut}^+(F)$. For a product of the free group of rank 2 on the same generators $F_2 = \langle x, y \rangle$, we have an embedding of $F_2 \times F_2$ into $\text{Aut}^+(F)$.

$$\begin{array}{ccc} F_2 \times F_2 : & \longrightarrow & \text{Aut}^+(F) \leq \text{Aut}(F) \\ (w_1, w_2) & \longmapsto & \widehat{w_1 w_2} \end{array},$$

Let $G = \langle x, y \mid R_1, \dots, R_m \rangle$ be a finitely presented group on two generators with unsolvable word problem (for example the group presented in [WXML14]). We then construct a group

$$A = \left\{ (\phi, \psi) \in F_2 \times F_2 \leq \text{Aut}^+(F) \mid \phi \stackrel{G}{=} \psi \right\} \leq F_2 \times F_2$$

As in Theorem 4, the group A is our action sub-group of $\text{Aut}(F)$ with unsolvable orbit decidability problem (since $\text{MP}(A, F_2 \times F_2)$ is unsolvable) and it is finitely generated:

$$A \cong \langle \phi_1 = (1, R_1), \dots, \phi_m = (1, R_m), \phi_{m+1} = (x, x), \phi_{m+2} = (y, y) \rangle$$

These generators get mapped into the copy of $F_2 \times F_2$ in $\text{Aut}^+(F)$:

$$A \cong \langle \widehat{\phi_1} = \widehat{R_1}, \dots, \widehat{\phi_m} = \widehat{R_m}, \widehat{\phi_{m+1}} = \widehat{x\hat{x}}, \widehat{\phi_{m+2}} = \widehat{y\hat{y}} \rangle$$

Let $F_n = \langle t_1, \dots, t_n \rangle$ be the free group of rank n (free groups have solvable conjugacy problem and $[C_{F_n} : a] = 1$, for $a \in F_n$). The group G given by the following presentation:

$$G = \left\langle \alpha, \beta, t_1, \dots, t_n \left| \begin{array}{l} [\alpha\beta^{-1}, \alpha^{-1}\beta\alpha], [\alpha\beta^{-1}, \alpha^{-2}\beta\alpha^2], \\ t_j^{-1}\alpha t_j = \widehat{\phi_j}^{-1}\alpha\widehat{\phi_j}, \\ t_j^{-1}\beta t_j = \widehat{\phi_j}^{-1}\beta\widehat{\phi_j} \end{array} \right. \right\rangle, \quad (2)$$

$j = 1, \dots, n$, is an extension of Thompson group F with solvable word problem and unsolvable conjugacy problem.

4 Application to Cryptography

Definition 1 Let G be a group with a finite generating set S . The **growth function** $\gamma(n)$ is defined for every $n \in \mathbb{N}$ as the number of elements of G which are product of at most n elements of S .

The $\lim_{n \rightarrow \infty} \sqrt[n]{\gamma(n)}$ exists always [dLH00]. A finitely generated group is said to have **exponential growth** if the limit is positive, and **subexponential growth** if the limit is 0. Exponential growth property is very important when using groups as base for cryptographic algorithm implementation, because groups with exponential growth provide larger key space. It is also interesting to note that having exponential or sub-exponential growth is an intrinsic property of the group, that is, it does not depend upon the finite generating set [dLH00].

Proposition 4 Thompson group F has exponential growth.

Proof Consider words of F in the following form:

$$X_1^{\epsilon_1} X_0^{-1} X_1^{\epsilon_2} X_0^{-1} \dots X_0^{-1} X_1^{\epsilon_n},$$

where $\epsilon_1, \dots, \epsilon_n \in \mathbb{N}$. By using the infinite presentation of F we can move the X_0^{-1} to the right to obtain:

$$X_1^{\epsilon_1} X_2^{\epsilon_2} \dots X_n^{\epsilon_n} X_0^{-(n-1)} \quad (3)$$

Words of (5.1) are in their normal forms, therefore we get a different element of F for every different values of $\epsilon_1, \dots, \epsilon_n$. \square

Since Thompson group F is contained in its extensions, we have:

Corollary 2 Any extension of Thompson group F has exponential growth.

We have seen that the extensions of Thompson group F developed in the previous chapter have all the interesting properties to be a base of a crypto system (exponential growth, solvable word problem, unsolvable conjugacy problem). In this section we discuss a generic application of such extensions for public-key cryptography. The protocol that we are going to describe is due to Anshel, Anshel and Goldfeld [AAG99]. The only necessary requirement for the algorithm is the solvability of the word problem. The security of the protocol relies on the so called **simultaneous conjugacy problem**, which is harder than the conjugacy problem. It can be stated as follows:

$$\text{SCP}(G) = \{(x_1, \dots, x_n, y_1, \dots, y_n) \in G^{2n} \mid \exists g \in G; y_i = g^{-1} x_i g\}.$$

The following proposition is immediate:

Proposition 5 For a group G we have the following reduction:

$$\text{CP}(G) \leq_m \text{SCP}(G)$$

and so as a corollary:

Corollary 3 The simultaneous conjugacy problem is unsolvable for extensions of Thompson group F with unsolvable conjugacy problem.

Given s_1, \dots, s_m and t_1, \dots, t_n are elements of a group G . The protocol can be described as follows between two users A and B.

1. User A computes a random element $a \in G$ as a word in terms of s_1, \dots, s_m denoted by $a(s_1, \dots, s_m)$ and sends $a^{-1}t_1a, \dots, a^{-1}t_na$ to B.
2. User B computes a random element $b \in G$ as a word in terms of t_1, \dots, t_n denoted by $b(t_1, \dots, t_n)$ and sends $b^{-1}s_1b, \dots, b^{-1}s_mb$ to A.
3. A computes $a(b^{-1}s_1b, \dots, b^{-1}s_mb) = b^{-1}ab$.
4. B computes $b(a^{-1}t_1a, \dots, a^{-1}t_na) = a^{-1}ba$.

At this point, user A disposes of the private key $a^{-1}b^{-1}ab = [a, b]$ and user B the key $b^{-1}a^{-1}ba = [b, a] = [a, b]^{-1}$ and user B can easily compute $[a, b]$ sharing this way the same private secret with A. An adversary C observing the transmissions (1) and (2) is unable to figure out a and b unless he/she can solve the set of simultaneous conjugacy over G .

One may think of applying the same procedure to create extensions of B_n with solvable word problem and unsolvable conjugacy problem which makes a cryptographic protocol based on extensions of B_n more difficult to break. Recently Meneses and Ventura in [GMV14] proved that:

Theorem 8 *The twisted conjugacy problem is solvable for B_n .*

Dyer and Grossman extensively studied the automorphisms of B_n :

Theorem 9 (Dyer, Grossman [DG81]) $\text{Aut}(B_n) = \text{Inn}(B_n) \sqcup \text{Inn}(B_n).\epsilon$, where $\epsilon : B_n \rightarrow B_n$ is the automorphism which inverts the generators of B_n ($\sigma_i \rightarrow \sigma_i^{-1}$).

This means that given $\varphi \in \text{Aut}(B_n)$ and by the previous theorem, either $\varphi = \gamma_g, g \in B_n$ or $\varphi = \gamma_g.\epsilon, g \in B_n$, where γ_g is the conjugation map. Given a finitely generated subgroup $A = \langle \varphi_1, \dots, \varphi_m \rangle \leq \text{Aut}(B_n)$, for every $i = 1, \dots, m$ we have $\varphi_i = \gamma_{g_i} \epsilon^\alpha$ ($\alpha = 0$ or 1). With this, it is easy to see that for $u, v \in B_n$, deciding whether or not there $\varphi \in A$ and $g \in B_n$ such that $\varphi(u) = g^{-1}vg$ reduces to solving conjugacy problem in B_n , which is solvable:

Corollary 4 *Every finitely generated subgroup $A \leq \text{Aut}(B_n)$ is orbit decidable.*

Thus what we have applied on Thompson group F to obtain extensions with unsolvable conjugacy problem does not apply on the braid group B_n and we have:

Corollary 5 *All extensions of B_n that can be constructed under the conditions of Theorem 2 have solvable conjugacy problem.*

References

- [AAG99] Iris Anshel, Michael Anshel, and Dorian Goldfeld. An algebraic method for public-key cryptography. *Mathematical Research Letters*, 6:287–292, 1999.
- [BMV10] Oleg Bogopolski, Armando Martino, and Enric Ventura. Orbit decidability and the conjugacy problem for some extensions of groups. *Transactions of the American Mathematical Society*, 362(4):2003–2036, 2010.
- [BMV13] José Burillo, Francesco Matucci, and Enric Ventura. The conjugacy problem in extensions of Thompson’s group F . *arXiv preprint arXiv:1307.6750*, 2013.
- [Boo54] William W Boone. Certain simple, unsolvable problems of group theory. i. In *Indagationes Mathematicae (Proceedings)*, volume 57, pages 231–237. Elsevier, 1954.
- [Bri96] Matthew G Brin. The chameleon groups of Richards J. Thompson: automorphisms and dynamics. *Publications Mathématiques de l’IHÉS*, 84:5–33, 1996.
- [DG81] Joan L Dyer and Edna K Grossman. The automorphism groups of the braid groups. *American Journal of Mathematics*, pages 1151–1169, 1981.
- [dLH00] Pierre de La Harpe. *Topics in geometric group theory*. University of Chicago Press, 2000.
- [Fos14] Ariadna Fossas. Thompson’s group t , undistorted free groups and automorphisms of the flip graph. In *Extended Abstracts Fall 2012*, pages 45–49. Springer, 2014.
- [Fri69] AA Fridman. On the relation between the word problem and the conjugacy problem in finitely defined groups. 1969.
- [GMV14] Juan González-Meneses and Enric Ventura. Twisted conjugacy in braid groups. *Israel Journal of Mathematics*, 201(1):455–476, 2014.
- [Mik66] KA Mikhailova. The occurrence problem for direct products of groups. *Matematicheskii Sbornik*, 112(2):241–251, 1966.
- [MSU08] Alexei Myasnikov, Vladimir Shpilrain, and Alexander Ushakov. *Group-based cryptography*. Springer Science & Business Media, 2008.
- [Nov54] PS Novikov. On algorithmic unsolvability of the word problem. 1954.
- [Nov58] Petr Sergeevich Novikov. Unsolvability of the conjugacy problem in group theory. 1958.
- [Sho97] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing*, 26(5):1484–1509, 1997.
- [WXLL14] Xiaofeng Wang, Chen Xu, Guo Li, and Hanling Lin. Groups with two generators having unsolvable word problem and presentations of Mihailova subgroups. Technical report, Cryptology ePrint Archive, Report 2014.528, <http://eprint.iacr.org>, 2014.